

IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF TEXAS  
DALLAS DIVISION

CLERK US DISTRICT COURT  
NORTHERN DIST. OF TX  
FILED

2010 APR 14 AM 9:11

DEPUTY CLERK

UNITED STATES OF AMERICA

v.

DAVID ANTHONY EDWARDS (2)  
also known as DAVUS

§  
§  
§  
§  
§  
§

No. 3:09-CR-100-B

FACTUAL RESUME

Defendant David Anthony Edwards, the defendant's attorney Mick Mickelsen, and the United States of America (the government), agree that the following accurately states the elements of the offense and the facts relevant to the offense to which the defendant is pleading guilty:

Elements:

1. In order for Edwards to be convicted at trial of a violation of 18 U.S.C. §371 (18 U.S.C. §§1030(a)(5)(A)(i), 1030(a)(5)(B)(i), and §1030(a)(6)(A)), the United States would have to prove each of the following elements of the offense beyond a reasonable doubt:

First: Edwards and at least one other person made an agreement to commit the crime of [see below violations of 18 U.S.C. §1030] as charged in the indictment;

Second: Edwards knew the unlawful purpose of the agreement and joined in it willfully, that is, with the intent to further the unlawful purpose;

and

Third: One of the conspirators during the existence of the conspiracy knowingly committed at least one of the overt acts described in the indictment, in order to accomplish some object or purpose of the conspiracy.

2. The essential elements of a violation of 18 U.S.C. §§1030(a)(5)(A)(i), 1030(a)(5)(B)(i), and §1030(a)(6)(A) are as follows:

First: the defendant knowingly caused the transmission of a program, information, code, or command to a computer;

Second: as a result of the transmission, the defendant intentionally caused damage to a computer without authorization;

Third: the damage resulted in losses to one or more persons totaling at least \$5,000 in value at any time during a one-year period; and

Fourth: the computer damaged was used in interstate or foreign commerce or communication.

3. Edwards lived in Mesquite, Texas, in the Northern District of Texas, Dallas

Division. He maintained a server at his home, and operated the website kidindustries.net from at least August 2004 through October 2007.

4. Edwards and codefendant Thomas James Frederick Smith, known to Edwards as Z00k, agreed and assisted each other to transmit a program, information, code, or command to a protected computer to control the computers, disclose confidential information, or deface a webpage. Specifically, Edwards and Smith knowingly and intentionally did:

a. create a coded application file called NETTICK, which could be used to access

another person's computer without authorization and gain control over the computer;

b. access other persons' computers without authorization and transmit NETTICK;

c. through the NETTICK, cause the compromised computers (the botnet) to log onto an Internet Relay Chat (IRC) channel hosted on Edward's website kidindustries.net, and wait for commands;

d. control and command the botnet from the IRC channel hosted on kidindustries.net;

e. cause damage to computers and computer systems.

5. On or about August 14, 2006, using Edward's website kidindustries.net Smith commanded the bots and caused a portion of the botnet, including one compromised computer in the Northern District of Texas, to engage in a distributed denial of service attack by flooding an IP address at a Internet Service Provider located in the Northern District of Texas. Smith did this to demonstrate NETTICK's capabilities.

6. On or about September 26, 2006, Edwards and Smith accessed without authorization the T35.net user database. T35.net provided free and paid personal and business Internet web hosting services for hundreds of thousands of users. The T35.net user database contained confidential user identifications and passwords. Smith and Edwards downloaded the T35.net's user database containing hundreds of thousands of the confidential user identifications and passwords.

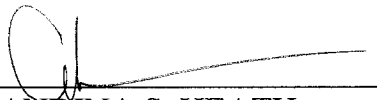
7. On or about October 3, 2006, Edwards, assisted by Smith, defaced the T35.net website and made the user identifications and passwords available to the public.

8. Edwards understands that compromising a computer causes damage or a loss to the particular individual whose computer was compromised.

9. Edwards understands that T35.net's cost to remediate the compromised database and server exceeded \$5,000.00, but was less than \$10,000.00.

Respectfully Submitted,

JAMES T. JACKS  
UNITED STATES ATTORNEY

  
CANDINA S. HEATH  
Assistant United States Attorney  
Texas State Bar No. 09347450  
1100 Commerce Street, Third Floor  
Dallas, Texas 75242-1699  
Tel: 214.659.8600  
Fax: 214.767.2846  
candina.heath@usdoj.gov


4-5-2010  
Date


I have read (or had read to me) this Factual Resume and have carefully reviewed every part of it with my attorney. I fully understand it and I swear that the facts contained herein are true and correct.



DAVID ANTHONY EDWARDS  
Defendant

2010-04-07  
Date

  
I am ~~Thomas James Frederick Smith~~'s counsel. I have carefully reviewed every part of this Factual Resume with my client. To my knowledge and belief, my client's decision execute this Factual Resume is an informed and voluntary one.

  
MICK MICKELSEN  
Attorney for Defendant Edwards

4-7-10  
Date